

Substitute for form 1449A/PTO

# INFORMATION DISCLOSURE STATEMENT BY APPLICANT

MAY 08 2006

Sheet

1

of

3

## Complete if Known

Application No.	10/698,814
Filing Date	October 30, 2003
First Named Inventor	Hugh S. Njemanze
Art Unit	2161
Examiner Name	Paul Kim
Attorney Docket Number	25137-11333

## U.S. PATENT DOCUMENTS

Examiner Initials*	Cite No. <sup>1</sup>	Document No. Number – Kind Code <sup>2</sup> (if known)	Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document
JK	A1	US-2004/0221191 A1	11-04-2004	Porras et al.
	A2	US-6,711,615	03-23-2004	Porras et al.
	A3	US-6,708,212	03-16-2004	Porras et al.
	A4	US-6,704,874 B1	03-09-2004	Porras et al.
	A5	US-2004/0024864 A1	02-05-2004	Porras et al.
	A6	US-2004/0010718 A1	01-15-2004	Porras et al.
	A7	US-2003/0093514 A1	05-15-2003	Valdes et al.
	A8	US-2003/0093692 A1	05-15-2003	Porras
	A9	US-2003/0101358 A1	05-29-2003	Porras et al.
	A10	US-6,484,203	11-19-2002	Porras et al.
	A11	US-6,321,338	11-20-2001	Porras et al.
	A12	US-5,717,919	02-10-1998	Kodavalla et al.

## FOREIGN PATENT DOCUMENTS

Examiner Initials*	Cite No. <sup>1</sup>	Foreign Patent Document Country Code <sup>3</sup> – Number <sup>4</sup> Kind Code <sup>5</sup> (if known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	T <sup>6</sup>

## OTHER REFERENCES – NON-PATENT LITERATURE DOCUMENTS

Examiner Initials*	Cite No. <sup>1</sup>	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published	T <sup>6</sup>
JK	C1	ARCSIGHT, "About ArcSight Team," date unknown, [online] [Retrieved on October 25, 2002] Retrieved from the Internet <URL: <a href="http://www.arcsight.com/about_team.htm">http://www.arcsight.com/about_team.htm</a> >.	
	C2	ARCSIGHT, "About Overview," October 14, 2002, [online] [Retrieved on April 21, 2006] Retrieved from the Internet <URL: <a href="http://web.archive.org/web/20021014041614/http://www.arcsight.com/about.htm">http://web.archive.org/web/20021014041614/http://www.arcsight.com/about.htm</a> >.	
	C3	ARCSIGHT, "Contact Info," date unknown, [online] [Retrieved on October 25, 2002] Retrieved from the Internet <URL: <a href="http://www.arcsight.com/contact.htm">http://www.arcsight.com/contact.htm</a> >.	

Examiner Signature	<i>Paul Kim</i>	Date Considered	8/5/2006
--------------------	-----------------	-----------------	----------

\*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609.

Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

<sup>1</sup>Applicant's unique citation designation number (optional). <sup>2</sup>See Kinds Codes of USPTO Patent Documents at [www.uspto.gov](http://www.uspto.gov) or MPEP 901.04. <sup>3</sup>Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). <sup>4</sup>For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. <sup>5</sup>Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST. 16 if possible. <sup>6</sup>Applicant is to place a check mark here if English language Translation is attached.

25137/11333/DOCS/1617974.1

**INFORMATION DISCLOSURE  
STATEMENT BY APPLICANT****Complete if Known**

Application No.	10/698,814
Filing Date	October 30, 2003
First Named Inventor	Hugh S. Njemanze
Art Unit	2161
Examiner Name	Paul Kim
Attorney Docket Number	25137-11333

Sheet

2

of

3

**OTHER REFERENCES – NON-PATENT LITERATURE DOCUMENTS**

Examiner Initials*	Cite No. <sup>1</sup>	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published	T <sup>6</sup>
<i>yk</i>	C4	ARCSIGHT, "Enterprise Coverage: Technology Architecture," date unknown, [online] Retrieved from the Internet <URL: <a href="http://www.snaiso.com/Documentation/Arcsight/arcsight_archtda.pdf">http://www.snaiso.com/Documentation/Arcsight/arcsight_archtda.pdf</a> >.	
	C5	ARCSIGHT, "Managed Process: ArcSight Reporting System," date unknown, [online] Retrieved from the Internet <URL: <a href="http://www.snaiso.com/Documentation/Arcsight/arcsight_reportsys.pdf">http://www.snaiso.com/Documentation/Arcsight/arcsight_reportsys.pdf</a> >.	
	C6	ARCSIGHT, "Managed Process: Console-Based Management," date unknown, [online] Retrieved from the Internet <URL: <a href="http://www.snaiso.com/Documentation/Arcsight/arcsight_console.pdf">http://www.snaiso.com/Documentation/Arcsight/arcsight_console.pdf</a> >.	
	C7	ARCSIGHT, "Precision Intelligence: SmartRules™ and Cross-Correlation," date unknown, [online] Retrieved from the Internet <URL: <a href="http://www.snaiso.com/Documentation/Arcsight/arcsight_correlation.pdf">http://www.snaiso.com/Documentation/Arcsight/arcsight_correlation.pdf</a> >.	
	C8	ARCSIGHT, "Precision Intelligence: SmartAgent™," date unknown, [online] Retrieved from the Internet <URL: <a href="http://www.ossmanagement.com/SmartAgent.pdf">http://www.ossmanagement.com/SmartAgent.pdf</a> >.	
	C9	ARCSIGHT, "Product Info: Product Overview and Architecture," date unknown, [online] [Retrieved on October 25, 2002] Retrieved from the Internet <URL: <a href="http://www.arcsight.com/product.htm">http://www.arcsight.com/product.htm</a> >.	
	C10	ARCSIGHT, "Product Info: 360° Intelligence Yields Precision Risk Management," date unknown, [online] [Retrieved on October 25, 2002] Retrieved from the Internet <URL: <a href="http://www.arcsight.com/product_info01.htm">http://www.arcsight.com/product_info01.htm</a> >.	
	C11	ARCSIGHT, "Product Info: ArcSight SmartAgents," October 10, 2002, [online] [Retrieved on April 21, 2006] Retrieved from the Internet <URL: <a href="http://web.archive.org/web/20021010135236/http://www.arcsight.com/product_info02.htm">http://web.archive.org/web/20021010135236/http://www.arcsight.com/product_info02.htm</a> >.	
	C12	ARCSIGHT, "Product Info: ArcSight Cross-Device Correlation," date unknown, [online] [Retrieved on October 25, 2005] Retrieved from the Internet <URL: <a href="http://www.arcsight.com/product_info03.htm">http://www.arcsight.com/product_info03.htm</a> >.	
	C13	ARCSIGHT, "Product Info: ArcSight Manager," date unknown, [online] [Retrieved on October 25, 2002] Retrieved from the Internet <URL: <a href="http://www.arcsight.com/product_info04.htm">http://www.arcsight.com/product_info04.htm</a> >.	
	C14	ARCSIGHT, "Product Info: ArcSight Console," date unknown, [online] [Retrieved on November 15, 2002] Retrieved from the Internet <URL: <a href="http://www.arcsight.com/product_info05.htm">http://www.arcsight.com/product_info05.htm</a> >.	
	C15	ARCSIGHT, "Product Info: ArcSight Reporting System," date unknown, [online] [Retrieved on October 25, 2002] Retrieved from the Internet <URL: <a href="http://www.arcsight.com/product_info06.htm">http://www.arcsight.com/product_info06.htm</a> >.	
	C16	ARCSIGHT, "Product Info: Enterprise Scaling," date unknown, [online] [Retrieved on October 25, 2002] Retrieved from the Internet <URL: <a href="http://www.arcsight.com/product_info07.htm">http://www.arcsight.com/product_info07.htm</a> >.	
	C17	ARCSIGHT, "Security Management for the Enterprise," 2002, [online] [Retrieved on October 25, 2002] Retrieved from the Internet <URL: <a href="http://www.arcsight.com/">http://www.arcsight.com/</a> >.	
	C18	ARCSIGHT, "Technical Brief: How Correlation Eliminates False Positives," date unknown, source unknown.	
	C19	BURLESON, D., "Taking Advantage of Object Partitioning in Oracle®i," November 8, 2000, [online] [Retrieved on April 20, 2004] Retrieved from the Internet <URL: <a href="http://www.dba-oracle.com/art_partit.htm">http://www.dba-oracle.com/art_partit.htm</a> >.	
<i>✓</i>	C20	DERODEFF, C., "Got Correlation? Not Without Normalization," 2002, [online] Retrieved from the Internet <URL:	

Examiner Signature	<i>Paul Kim</i>	Date Considered	8/3/2006
--------------------	-----------------	-----------------	----------

\*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609.

Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

<sup>1</sup>Applicant's unique citation designation number (optional). <sup>2</sup>See Kinds Codes of USPTO Patent Documents at [www.uspto.gov](http://www.uspto.gov) or MPEP 901.04. <sup>3</sup>Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). <sup>4</sup>For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. <sup>5</sup>Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST. 16 if possible. <sup>6</sup>Applicant is to place a check mark here if English language Translation is attached.

25137/11333/DOCS/1617974.1

**INFORMATION DISCLOSURE  
STATEMENT BY APPLICANT****Complete if Known**

Application No.	10/698,814
Filing Date	October 30, 2003
First Named Inventor	Hugh S. Njemanze
Art Unit	2161
Examiner Name	Paul Kim
Attorney Docket Number	25137-11333

Sheet

3

of

3

**OTHER REFERENCES – NON-PATENT LITERATURE DOCUMENTS**

Examiner Initials*	Cite No. <sup>1</sup>	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published	T <sup>2</sup>
YK		<a href="http://www.svic.com/papers/pdf/Got-Correlation_rmalization.pdf">http://www.svic.com/papers/pdf/Got-Correlation_rmalization.pdf</a> .	
YK	C21	CHEUNG, S. et al., "EMERALD Intrusion Incident Report: 601 Message Specification," August 10, 2000, System Design Laboratory, SRI International.	
	C22	National Institute of Standards and Technology (NIST), "Federal Information Processing Standards Publication (FIPS PUB) 199: Standards for Security Categorization of Federal Information and Information Systems", February 2004.	
	C23	Haley Enterprise, "Production Systems," 2002, [online] [Retrieved on October 29, 2002] Retrieved from the Internet <URL: <a href="http://www.haley.com/0072567836705810/ProductionSystems.html">http://www.haley.com/0072567836705810/ProductionSystems.html</a> >.	
	C24	Haley Enterprise, "The Rete Algorithm," 2002, [online] [Retrieved on October 29, 2002] Retrieved from the Internet <URL: <a href="http://www.haley.com/0072567836705810/ReteAlgorithm.html">http://www.haley.com/0072567836705810/ReteAlgorithm.html</a> >.	
	C25	Haley Enterprise, "A Rules Engine for Java Based on the Rete Algorithm," 2002, [online] [Retrieved on October 29, 2002] Retrieved from the Internet <URL: <a href="http://www.haley.com/0072567836705810/ReteAlgorithmForRules.html">http://www.haley.com/0072567836705810/ReteAlgorithmForRules.html</a> >.	
	C26	HALME, L.R. et al., "AINT Misbehaving: A Taxonomy of Anti-Intrusion Techniques," 2000, [online] [Retrieved on November 1, 2002] Retrieved from the Internet <URL: <a href="http://www.sans.org/newlook/resources/IDFAQ/aint.htm">http://www.sans.org/newlook/resources/IDFAQ/aint.htm</a> >.	
	C27	LINDQVIST, U. et al., "Detecting Computer and Network Misuse Through the Production-Based Expert System Toolset (P-BEST)," Proceedings of the IEEE Symposium on Security and Privacy, Oakland, California, May 9-12, 1999.	
	C28	CERT Coordination Center, "Overview of Attack Trends," 2002, [online] Retrieved from the Internet <URL: <a href="http://www.cert.org/archive/pdf/attack_trends.pdf">http://www.cert.org/archive/pdf/attack_trends.pdf</a> >.	
	C29	PORRAS, P.A. et al., "EMERALD: Event Monitoring Enabling Responses to Anomalous Live Disturbances," October 1997, Proceedings of the 20 <sup>th</sup> NIST-NCSC National Information Systems Security (NISS) Conference.	
	C30	PORRAS, P.A. et al., "A Mission-Impact-Based Approach to INFOSEC Alarm Correlation," October 2002, Lecture Notes in Computer Science, Proceedings: Recent Advances in Intrusion Detection, pp. 95-114, Zurich, Switzerland.	
	C31	INGARGIOLA, G., "The Rete Algorithm," date unknown, [online] [Retrieved on October 29, 2002] Retrieved from the Internet <URL: <a href="http://yoda.cis.temple.edu:8080/UGAIWWW/lectures/rete.html">http://yoda.cis.temple.edu:8080/UGAIWWW/lectures/rete.html</a> >.	
	C32	BRUNEAU, G., "What Difficulties are Associated on Matching Events with Attacks. Why is Event/Data Correlation Important?," 2001, [online] [Retrieved on November 1, 2002] Retrieved from the Internet <URL: <a href="http://www.sans.org/newlook/resources/IDFAQ/matching.htm">http://www.sans.org/newlook/resources/IDFAQ/matching.htm</a> >.	
	C33	National Institutes of Health (NIH), "Table 1: Security Categorization of Federal Information and Information Systems," revised July 8, 2005, [online] [retrieved on April 6, 2006] Retrieved from the Internet <URL: <a href="http://irm.cit.nih.gov/security/table1.htm">http://irm.cit.nih.gov/security/table1.htm</a> >.	
↓	C34	WOOD, M., et al., "Internet-Draft: Intrusion Detection Message Exchange Requirements," June 23, 2002, [online] [Retrieved on November 1, 2002] Retrieved from the Internet <URL: <a href="http://www.silicondefense.com/idwg/draft-ietf-idwg-requirements-07.txt">http://www.silicondefense.com/idwg/draft-ietf-idwg-requirements-07.txt</a> >.	

Examiner  
Signature

Youn / L

Date  
Considered

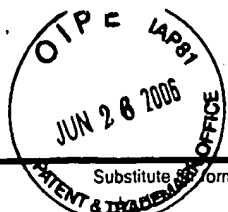
6/3/2006

\*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609.

Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

<sup>1</sup>Applicant's unique citation designation number (optional). <sup>2</sup>See Kinds Codes of USPTO Patent Documents at [www.uspto.gov](http://www.uspto.gov) or MPEP 901.04. <sup>3</sup>Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). <sup>4</sup>For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. <sup>5</sup>Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST. 16 if possible. <sup>6</sup>Applicant is to place a check mark here if English language Translation is attached.

25137/11333/DOCS/1617974.1



Substitute Form 1449A/PTO		<b>Complete if Known</b>	
<b>INFORMATION DISCLOSURE STATEMENT BY APPLICANT</b>		Application No.	10/698,814
		Filing Date	October 30, 2003
		First Named Inventor	Hugh S. Njemanze
		Art Unit	2161
		Examiner Name	Paul Kim
Sheet 1 of 1	Attorney Docket Number	25137-11333	

U.S. PATENT DOCUMENTS				
Examiner Initials*	Cite No. <sup>1</sup>	Document No. Number - Kind Code <sup>2</sup> (if known)	Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document
yk	A1	US-2005/0204404 A1	09-15-2005	Hrabik et al.
↓	A2	US-6,988,208	01-17-2006	Hrabik et al.
↓	A3	US-2002/0099958 A1	07-25-2002	Hrabik et al.

FOREIGN PATENT DOCUMENTS					
Examiner Initials*	Cite No. <sup>1</sup>	Foreign Patent Document Country Code <sup>3</sup> - Number Kind Code <sup>5</sup> (if known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	T <sup>6</sup>
jk	B1	WO 02/060117 A1	08-01-2002	Solutionary, Inc.	

OTHER REFERENCES – NON-PATENT LITERATURE DOCUMENTS				
Examiner Initials*	Cite No. <sup>1</sup>	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published	T <sup>6</sup>	

Examiner Signature	<i>Paul Kim</i>	Date Considered	8/3/2006
--------------------	-----------------	-----------------	----------

\*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609.

Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

<sup>1</sup>Applicant's unique citation designation number (optional). <sup>2</sup>See Kinds Codes of USPTO Patent Documents at [www.uspto.gov](http://www.uspto.gov) or MPEP 901.04. <sup>3</sup>Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). <sup>4</sup>For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. <sup>5</sup>Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST. 16 if possible. <sup>6</sup>Applicant is to place a check mark here if English language Translation is attached.

25137/11333/DOCS/1633620.1